Trinity Grammar School

MIND

BODY SPIRIT

INFORMATION & COMMUNICATION TECHNOLOGY STUDENT ACCEPTABLE USE AGREEMENT

YEARS 7 – 12

Introduction/Rationale

As a Trinity Grammar School (TGS) student, you will have access to wide-ranging computer facilities within the School. Access to the School's computing and network facilities is a privilege.

The School recognises that students will use a range of communication devices, resources and services, both School owned and student-owned.

Boys are expected to use all ICT devices, resources and services responsibly, purposefully and ethically. Any activities that impact adversely on users inside or outside the School, or that adversely affect the School's reputation, will be considered a serious breach of the School's rules.

Usage of devices, services and resources is always at the discretion of class teachers and other School staff.

The School acknowledges that there is some material on the Internet which is inappropriate for the boys of this School. We recognise that we have a duty of care to promote the suitable use of the Internet. However, neither the information, nor the content of such information on the Internet, can be controlled by the School. Further, it is technically impossible to simultaneously grant access to Internet resources while completely blocking inappropriate or controversial material.

Student Responsibilities

In order to ensure that students use the Internet in a safe and responsible manner and to ensure that there is continued availability and equity of access to the School's ICT facilities, all students need to agree to and adhere to the following:

1. All boys are expected to take personal responsibility for the security of their device at all times on campus and to bring their device charged and ready for use to class ready to learn, unless an instruction to the contrary has been issued by a class teacher:
    - Other than in a locked School locker, devices should never be left unattended when not in use.
    - Boys need to rectify any login or technical issues promptly and not during class time.
    - Notify a teacher if you believe that you have identified a security problem or any other problem with the School's network.

2. All boys are expected to carefully manage their data and their online identity:
    - Passwords should never be written down at school and or given to another person; students will be held responsible for all activity undertaken using their login/password. It is wise to keep a record of your passwords at home in a secure location.
    - Although the School takes care to backup server-based resources, keeping backups of critical files (e.g. assignment work) is each boy's responsibility.
    - Do not reveal personal details such as PINs, addresses, passwords, date of birth and account details.

- Use social networking sites in a responsible and cyber safe manner by not revealing personal details, by restricting access to your social networking pages only to people whom you know and can trust and by not posting offensive or harassing information on the sites.

3. All boys are expected to act with integrity, and while at School use ICT devices, resources and services for educational purposes:
    - Students should respect the holders of copyright and not break copyright law, never plagiarise the work of others and always use appropriate referencing systems;
    - Boys must not access or attempt to access inappropriate sites or resources;
    - As with other non-ICT areas, vandalism is always inappropriate;
    - Unless specifically allowed by a teacher for educational purposes, the sending and receiving of text messages or phone calls and the use of social networking sites, gaming and services (eg. Facebook) are strictly prohibited during scheduled school time.
    - All modes of electronic communication must be used with integrity by being honest, sensitive to others and reliable in what you communicate.
    - Boys may not use personal 3G/4G mobile broadband "hot spots" to provide alternate Internet connections.
    - Do not use the School's Internet network for chatting or social networking under any circumstances without the consent of a teacher for School related purposes.

4. Boys are expected to treat others with respect and ensure the rights and privacy of others are maintained:
    - It is never acceptable to digitally record (by photo, audio or video) boys or teachers, or distribute that information without permission from that person and your class teacher;
    - Do not access or send information that may be considered offensive, inappropriate or anti-social in our School environment such as profane messages to other students, hurtful comments, pornographic photographs or photographs that have been changed or altered to make fun of others;
    - Boys must not access or try to gain access to private or sensitive information or the account of another boy or member of School staff;
    - The equipment and services of the School and other boys should always be treated with care and respect;
    - Boys are expected to follow appropriate etiquette and protocols when communicating with staff, other students, and those outside the School;
    - Harassment of others when using the Internet or other communication devices such as mobile phones at School, home or any other location is not acceptable. (Harassment includes but is not limited to physical, verbal or psychological behaviour which makes another person feel embarrassed, offended, upset, devalued, degraded, afraid, frustrated or angry. More specifically, harassment using IT devices includes, but is not limited to, the sending of unwarranted messages or messages that are derogatory, defaming or hurtful via e-mails, text messages; posting comments on blogs, on social networking sites, in chat rooms or on other websites, SMS, MMS messages and other approved and non-approved modes of electronic communication.);
    - Respect for the School and its reputation is paramount. Boys must not make comments on the Internet or send comments via any electronic communication device that could hurt the reputation of Trinity Grammar School.
    - Impersonation of others when using the Internet is not acceptable;
    - Boys must not log on using someone else's account;
    - Boys must act responsibly regarding the taking of photographs and videos, the sending of these using electronic devices and the posting of them on the Internet. It is expected that students will:
        - Not take photographs or videos at School or School related functions, tours or activities without the permission of a teacher.
        - Not distribute or post photographs, graphical images or videos of students, teachers or their relatives on the Internet without the permission of the particular student, teacher or relative of the student or teacher.
        - Seek the express permission of those photographed before forwarding images to other persons or posting such images online.

If students are harassed online they should:

- Avoid retaliating or responding.
- Print or screenshot the offending material and turn off the device, give a copy to their parent and/or a member of staff and discuss with their parent or teacher the harassment before taking action.
- Block the bully and change their privacy settings.
- Report abuse to the social media service.
- Incidents should be reported to a teacher or the Master of the Preparatory, Junior, Middle or Senior Schools if the harassment involves other students, teachers or members of the Trinity community.
- If they continue to be cyberbullied and they believe it is having a serious threatening, intimidating, harassing or humiliating effect, make an online complaint to the Children's Safety Commissioner using the Commissioner's website - https://esafety.gov.au/complaints-and-reporting
- The matter could also be referred to the police.

Consequences

The School reserves the right to confiscate and to review the contents of any ICT device (such as electronic tablets or notebooks, personal mobile phones, iPads, iPods, MP3 players, computers, USB or other electronic personal devices), suspected of being used inappropriately at School or School events. The School will keep confiscated devices for the duration of any subsequent investigation. Boys must agree to give access to the confiscated devices and to give their password to a senior member of staff.

Consequences for students who break this agreement may include, but are not limited to, warnings, reprimands, cancellation of access privileges to the School's network facilities, detentions, suspension from school and in cases of gross or repeated violations of the agreement students may be expelled.

Related Documents

These documents are found in the Record Book and School Handbook and are related to the ICT Student Acceptable Use Agreement or directly referenced by it.

http://community.trinity.nsw.edu.au/global_docs/handbook.pdf

- A Safe Learning & Working Environment | Page 47
- Discipline System: Pre-K to 12 | Page 50
- School Expectations | Page 55

These documents also relate to the ICT Student Acceptable Use Agreement and are found on the School's Website:

- **TGS BYOD Device Specifications Years 5-6**
- **TGS BYOD Device Specifications Years 7-12**

Supervision and Monitoring

School

The use of School-owned information technology resources is not private. School and network administrators and other appropriate staff monitor the use of information technology resources to help ensure that uses are secure and appropriate. The School reserves the right to examine, use, and disclose any data found on the School's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to the police.

The School reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The School also reserves the right to limit the time of access and priorities among competing acceptable uses.

Liability and Insurance

The School will not be responsible for damage or harm to persons, files, data, or hardware. While the School employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. The School will not be responsible, financially or otherwise, for unauthorised transactions conducted over the School network.

School Devices

A student/family will be responsible to reimburse the School for repair or replacement of any School device that is damaged, lost or stolen whilst on loan to the particular student.

BYOD

The School does not accept liability for any loss, damage or theft of any device that is brought to school under the BYOD programme. The responsibility for the storage, safe-keeping and care of the device is the responsibility of the device owner. The School insurance policy does not apply to these devices; instead these should be covered by the user's insurance policy. As such it is strongly recommended that families ensure that details such as serial numbers and receipts of purchase for these devices are stored securely at home for insurance purposes.